ABSTRACT

Methods and apparatus for an encryption processor for performing accelerated computations to establish secure network sessions. The encryption processor includes an execution unit and a decode unit. The execution unit is configured to execute Montgomery and Montgomery operations and including at least one adder and at least two multipliers. The decode unit is configured determine if a square operation or a product operation needs to be performed and to issue the appropriate instructions so that certain multiply and/or addition operations are performed in parallel in the execution unit while performing the either the Montgomery square or Montgomery product operation.